

身份证地址均来自同一个县城，一前一后进入银行网点却互称不认识对方，开卡过程中眼神交流频繁，执意开通较大转账额度却不配合尽职调查……林某和王某的一系列异常举动引起了银行网点工作人员的警觉。经警银密切联动多方排查后，商业银行网点成功拦截了林某和王某的异常开户行为。

近年来，为了有效堵截非法资金转移，商业银行加强了银行账户(含卡)事前事中事后的全生命周期管理，事前强化尽职调查、事中加强风险监测和银警协作，事后进行客户回访、排查清理存量账户等，建立了防控不法分子利用银行账户转移非法资金的防护网，在协助公安机关打击治理电信网络诈骗方面取得了明显成效。

数据显示，2021年，电信网络诈骗犯罪分子利用单位银行账户转移资金的账户数量同比下降92%，个人银行卡户均涉案金额下降22%，商业银行协助公安机关止付、冻结涉诈资金同比增长270%，挽回大量群众损失。

金融机构筑牢风险防线

公安机关“断卡”行动开展以来，人民银行组织商业银行会同公安机关建立了密切的警银协作机制，筑牢不法分子恶意开卡的风险防控壁垒，有效防范不法分子到商业银行开卡后用于转移电信网络诈骗资金。商业银行网点一旦发现恶意开卡、买卖银行卡的可疑人员，将第一时间向辖区公安机关反映情况，公安机关快速排查、立即出警抓捕可疑人员，让恶意到商业银行开卡的不法分子“自投罗网”。

2021年7月，兴业银行哈尔滨分行发现了林某和王某的异常行为后，第一时间与当地反诈中心联系，反诈中心仅用1分钟便锁定王某近期开通多张手机卡和银行卡，行为极其异常。公安机关立即出警，联动银行网点成功拦截此次异常开卡行为。

为确保以点带面、连根铲除风险，人民银行哈尔滨中心支行在公安机关的协助下，组织商业银行对林某和王某可疑开卡行为进行排查。经排查，2006年10月至2021年7月，王某在黑龙江省内10家银行开立借记卡、贷记卡、准贷记卡等25个账户，频繁开销账户行为符合公安机关“断卡”行动可疑特征。各相关商业银行提高了王某的客户风险等级，将有关可疑交易线索提供给公安机关。

为深入推进打击治理电信网络诈骗犯罪，多部门联合以“零容忍”态度严厉打击买卖、租借银行卡活动，对非法开卡、办卡、贩卡团伙和诈骗分子形成有力震慑。一方面，根据《中华人民共和国刑法》规定，明知他人利用信息网络实施犯罪，为其犯罪提供支付结算帮助的，将构成“帮助信息网络犯罪活动罪”，需承担相应的法律责任。另一方面，根据《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》(银发〔2019〕85号)规定，公安部、人民银行将对买卖账户单位或个人严格审慎实施5年内暂停其银行账户非柜面业务、支付账户

所有业务，并不得为其新开立账户的金融惩戒。惩戒期满后，受惩戒的单位和个人办理新开立账户业务的，商业银行和支付机构还要加大审核力度。

此外，商业银行、支付机构、清算机构为了阻断电信网络诈骗资金非法转移，不断提升风险防控水平。商业银行和支付机构对公安机关通报的涉案银行卡严格实施“一案双查”，逐户倒查涉案账户的关联账户，依法向公安机关移送大量线索。中国银联组织各商业银行开展银行卡清理整治，全面清理长期不动银行卡和“一人多卡”，大幅降低了不法分子盘活存量银行卡的风险。中国银联研究建立了跨机构风险防控机制，推进“一键查卡”试点，在便利个人银行卡信息查询的同时，有效防范冒名开户风险。

电信网络诈骗涉案资金转移手法揭秘

当前电信网络诈骗犯罪高发多发，作案手段变化快、迷惑性强、防范难度大，诈骗窝点加速向境外转移，有组织犯罪特征日趋明显，严重破坏社会稳定和人民群众财产安全。

根据相关人士介绍，从涉案资金转移手法看，主要分为三个环节。

首先是收款环节：买卖、租借银行卡收取诈骗资金。犯罪分子主要通过购买、租用他人实名开立的银行卡、支付账户收取被害人资金。据公安部门通报，2021年1至11月，共破获电信网络诈骗案件37万起，打掉涉“两卡”违法犯罪团伙3.9万个，涉案银行卡全部为实名开立后非法买卖。

二是转移环节：账户层层嵌套、资金多方划转。诈骗分子为躲避公安机关止付、冻结措施，往往快速转移涉案资金，目前主要有三种方式。一是通过境内“水房”（洗钱团伙）实施转移。境内组建洗钱工作室专门从事诈骗资金转移，形成境外人员实施诈骗、通过聊天软件指挥境内“水房”快速转移洗白资金的黑色产业链。二是“跑分平台”拆分交易。资金通过“跑分平台”等非法支付平台进行大量拆分，转移至普通群众受高额利诱实名开立的银行卡、支付账户。三是利用虚拟货币转移赃款。诈骗分子通过购买虚拟货币向境外转移涉诈资金，查控难度大。

最后是变现环节：资金跨境转移变现。为规避打击，诈骗分子通常隐藏在境外，通过地下钱庄将境内的诈骗资金转移出境完成变现。一是刷卡取现。雇佣境内“车手”在银行ATM取现后非法走私出境，或者通过非法改装移机境外的POS机刷卡取现。二是虚构交易。构造虚假交易实现诈骗资金跨境转移，如签订虚假贸易合同，或者购买游戏点卡、充值卡等虚拟商品后转卖完成变现。三是跨境“对敲”。通过地下钱庄境内交割人民币、境外交割外币等方式，实现诈骗资金跨境转移。

在电信网络诈骗形势严峻背景下，人民银行加强顶层设计和工作部署，联合有关部门印发《电信网络诈骗和跨境赌博“资金链”治理工作方案》，提出29项具体工作措施，提升打击治理工作的整体性、系统性；出台《关于加强支付受理终端及相关业务管理的通知》，强化收款条码管理，重拳打击“跑分平台”；推动出台《非银行支付机构条例》，对参与电信网络诈骗、为不法分子提供便利的非银行支付机构严肃处罚。

人民银行表示，下一步将继续全力协助公安机关打击治理电信网络诈骗，持续压实金融机构风险防控责任，推进行业风险整治，促进跨机构、跨市场、跨部门的风险共享和协同处置，构建全链条齐抓共管格局，织密金融风险防控网，牢牢守住人民群众的“钱袋子”。

来源：中新网